Shembulli 1: msg="ALAN_TURING" çelësi="ENIGMA"

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_	A	B	C	D
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_	A	B	C	D	E	F	G	H	I	J	K	L	M
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_	A	B	C	D	E	F	G	H
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_	A	B	C	D	E	F
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_	A	B	C	D	E	F	G	H	I	J	K	L
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_

A L A N _ T U R I N G
E N I G M A E N I G M
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
E Y I T L T Y D Q T S → mesazhi i kriptuar

E N I G M A E N I G M
E Y I T L T Y O Q T S
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
A L A N _ T U R I N G → mesazhi i dekriptuar

19204234

Shembulli:

mesazhi: "KRIPTOSISTEMET"

çelësi: "PUBLIK"

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

K R I P T O S I S T E M E T

P U B L I K P U B L I K P U

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

Z L J A B Y H C T E P W T N — mesazhi i kriptuar

P U B L I K P U B L I K P U

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

Z L J A B Y H C T E P W T N

K R I P T O S I S T E M E T — mesazhi i dekriptuar

Lemball3: msg: "RIVEST-SHAMIR-ADLEMAN"
sekret: "RSA"

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z –
R S T U V W X Y Z – A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z –

RIVEST-SHAMIR-ADLEMAN
RSARSARSARSARSARSARSA
H-VVJTQJHROIHRAUCECSN

Mesaxli i kriptuar

RSARSARSARSARSARSARSA
H-VVJTQJHROIHRAUCECSN
RIVEST-SHAMIR-ADLEMAN

Mesaxli i dekriptuar

19204834

OTP

Shembulli: mesazhi: "INFORMATË", çelësi: "ÇELËS"

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Ë Ç
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27

m = 28

INFORMATË
08 13 05 14 17 12 00 19 26

ÇELËS
27 04 11 26 18

(+) mod(m)

08	13	05	14	17	12	00	19	26
27	04	11	26	18	27	04	11	26
07	17	16	12	07	11	04	02	24
H	R	Q	M	H	L	E	C	Y

Mesazhi i kriptuar

(-) mod(28)

07	17	16	12	07	11	04	02	24
27	04	11	26	18	27	04	11	26
08	13	05	14	17	12	00	19	26
I	N	F	O	R	M	A	T	Ë

Mesazhi i dekriptuar.

Alfabeti 2 =

A	B	C	D	E	Ë	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Ë
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	

[m = 27]

S	T	R	U	K	T	U	R	A	D	I	S	K	R	E	T	E		M	A	T	E	M	A	T	I	K	Ë
18	19	17	20	10	19	20	17	00	03	08	18	10	17	04	19	04		12	00	19	04	12	00	19	08	10	26

mesazhi i Kriptuar

mod(27)	18	19	17	20	10	19	20	17	00	03	08	18	10	17	04	19	04	
(+)	12	00	19	04	12	00	19	08	10	26	12	00	19	04	12	00	19	
	03	19	03	24	22	19	12	25	10	02	20	18	02	21	16	19	23	
	D	T	J	Y	W	T	M	Z	K	C	U	S	C	V	Q	T	X	

mesazhi i Dekriptuar

mod(27)	03	19	03	24	22	19	12	25	10	02	20	18	02	21	16	19	23	
(-)	12	00	19	04	12	00	19	08	10	26	12	00	19	04	12	00	19	
	18	19	17	20	10	19	20	17	00	03	08	18	10	17	04	19	04	
	S	T	R	U	K	T	U	R	A	D	I	S	K	R	E	T	E	

m = 26

KRIPTOSISTEMET ONETIMEPAD

mod(26) (+)

10, 17, 08, 15, 19, 14, 18, 08, 17, 19, 04, 17, 04, 19
14, 13, 04, 19, 08, 12, 04, 15, 00, 03, 14, 13, 04, 19

24 04 12, 08, 01, 00, 22, 23, 17, 22, 18, 04, 08, 12
Y E M I B A W X R W S E I M

Mesazhi i kriptuar

mod(26) (-)

24, 04, 12, 08, 01, 00, 22, 23, 17, 22, 18, 04, 08, 12
14 13, 04 19 08, 12, 04, 15, 00, 03, 14, 13, 04, 19

10, 17, 08, 15, 19, 14, 18, 08, 17, 19, 04, 17, 04, 19
K R I P T O S I S T E M E T

Mesazhi i dekriptuar

19204234

RSA-MATRICA

1) $p=3$, $q=11$, msg: "KRIPTOGRAFIA"

1) $m = 3 \cdot 11 = 33$
2) $\varphi(m) = 2 \cdot 10 = 20$
3) $e = ?$, $1 < e < 20$, $(e, 20) = 1$

$e = \{3, 5, 7, 9, 11, 13, 17, 19\}$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

K	R	I	P	T	O	G	R	A	F	I	A
10	17	8	15	19	14	6	17	0	5	2	0

$10^3 \equiv 10 \pmod{33}$

$17^3 \equiv 29 \pmod{33}$
$8^3 \equiv 17 \pmod{33}$
$15^3 \equiv 09 \pmod{33}$
$19^3 \equiv 28 \pmod{33}$
$14^3 \equiv 20 \pmod{33}$
$6^3 \equiv 18 \pmod{33}$
$17^3 \equiv 29 \pmod{33}$
$0^3 \equiv 0 \pmod{33}$
$5^3 \equiv 26 \pmod{33}$
$8^3 \equiv 17 \pmod{33}$
$0^3 \equiv 0 \pmod{33}$

10, 29, 17, 9, 28, 5, 18, 29, 0, 26, 17, 0

Mesarki i Knjituan

19204834

2

RSA

2. $p=5,\ g=13,\ e=7$

$n = 5 \cdot 13 = 65$

$\varphi(n) = 4 \cdot 12 = 48$

$7 \cdot d \equiv 1 \pmod{48}$

$d = 7$

$50^7 \equiv 15 \pmod{65}$ P

$43^7 \equiv 17 \pmod{65}$ R

$57^7 \equiv 08 \pmod{65}$ I

$25^7 \equiv 25 \pmod{65}$ Z

$43^7 \equiv 17 \pmod{65}$ R

$04^7 \equiv 04 \pmod{65}$ E

$52^7 \equiv 13 \pmod{65}$ N

$57^7 \equiv 08 \pmod{65}$ I

(1) $43 \equiv 43 \pmod{65}$

$43^6 \equiv 14 \pmod{65}$

$43^7 \equiv 17 \pmod{65}$

---

(2) $57^6 \equiv 57 \pmod{65}$

$57^6 \equiv 64 \pmod{65}$

3

RSA

3. $p=5, q=7, n=35, \varphi(n)=24, e=5$

5. $d \equiv 1 \pmod{24}$

$d=5$

$33^5 \equiv 03 \pmod{35}$ D

$00^5 \equiv 0 \pmod{35}$ A

$12^5 \equiv 17 \pmod{35}$ R

$33^5 \equiv 03 \pmod{35}$ D

$00^5 \equiv 00 \pmod{35}$ A

$13^5 \equiv 13 \pmod{35}$ N

$08^5 \equiv 08 \pmod{35}$ I

$00^5 \equiv 0 \pmod{35}$ A

$1920\,4823\,4$

$3913\,5393$

$2483\,832$

Matrica

Shembulli 4:

K O S O V A I M E
10 14 18 14 21 00 09 12 04

$l = 3 \cdot 3$

$$M = \begin{bmatrix} 10 & 14 & 08 \\ 14 & 21 & 12 \\ 18 & 00 & 04 \end{bmatrix} \quad K = \begin{bmatrix} 1 & 3 & 5 \\ -2 & -3 & 1 \\ 1 & 2 & -5 \end{bmatrix}$$

$$X = \begin{bmatrix} 10 & 14 & 08 \\ 14 & 21 & 12 \\ 18 & 00 & 04 \end{bmatrix} \times \begin{bmatrix} 1 & 3 & 5 \\ -2 & -3 & 1 \\ 1 & 2 & -5 \end{bmatrix} = \begin{bmatrix} 142 & 72 & 64 \\ -44 & -31 & -48 \\ -52 & 56 & 12 \end{bmatrix}$$

minorët

K^{-1}

$$M = \begin{bmatrix} -13/19 & -25/19 & -18/19 \\ 9/19 & 10/19 & 11/19 \\ 1/19 & -11/19 & -3/19 \end{bmatrix} \times \begin{bmatrix} 142 & 72 & 64 \\ -44 & -31 & -48 \\ -52 & 56 & 12 \end{bmatrix} = \begin{bmatrix} 10 & 14 & 08 \\ 14 & 21 & 12 \\ 18 & 00 & 04 \end{bmatrix}$$

kofaktorët

Exemplu 5:

D A R D A N
03 00 14 03 00 13

$l = 3 \cdot 2$

$$M = \begin{bmatrix} 03 & 03 \\ 00 & 00 \\ 14 & 13 \end{bmatrix} \qquad A = \begin{bmatrix} 5 & 3 & 1 \\ 1 & -3 & -2 \\ -5 & 2 & 1 \end{bmatrix}$$

$$K = A^2 + I = \begin{bmatrix} 23 & 08 & 00 \\ 12 & 08 & 05 \\ -28 & -19 & -8 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \Rightarrow$$

$$K = \begin{bmatrix} 24 & 08 & 0 \\ 12 & 09 & 5 \\ -28 & -19 & -7 \end{bmatrix}$$

$$X = \begin{bmatrix} 24 & 08 & 00 \\ 12 & 09 & 05 \\ -28 & -19 & -7 \end{bmatrix} \times \begin{bmatrix} 03 & 03 \\ 00 & 00 \\ 14 & 13 \end{bmatrix} = \begin{bmatrix} 72 & 72 \\ 106 & 101 \\ -182 & -175 \end{bmatrix}$$

72, 106, −182, 72, 101, −175

Mesajul i Kriptează

Matrici

Rhombulli : 6

M = ?

$$X = \underset{3\times 6}{\begin{bmatrix} -154 & -138 & -142 & -150 & -177 & -76 \\ 30 & 22 & 33 & 41 & 35 & 16 \\ 172 & 156 & 146 & 154 & 194 & 84 \end{bmatrix}}$$

$$K = \begin{bmatrix} -3 & -3 & 4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} -1/31 & -24/31 & 7/31 \\ -4/31 & 28/31 & -3/31 \\ 4/31 & 3/31 & 3/31 \end{bmatrix}$$

$$M = K^{-1} \times X = \begin{bmatrix} ? \\ \cdot \end{bmatrix}$$